

**REMARKS**

Please reconsider the application in view of the above amendments and the following remarks.

**Claim for Priority**

Applicant respectfully requests that the Examiner acknowledge the claim for priority. The present application claims priority to European Patent application EP 02292180.3 filed on September 4, 2002 and PCT Application PCT/IB2003/003577 filed on August 28, 2003.

**Disposition of claims**

Claims 1 – 6 were pending in this application. Claim 3 has been canceled without disclaimer or prejudice. New claim 7 has been added by way of this reply. Claims 1, 5, 6, and 7 are independent. Claims 2 and 4 depend, directly or indirectly, from independent claim 1. Thus, claims 1, 2, 4 – 7 are now pending in this application.

**Claim amendments**

Claims 1, 2, 4, 5, and 6 have been amended by way of this reply to further clarify the claimed invention. Support for this amendment may be found, for example, in paragraphs [0023] – [0025] of the publication of the Specification.

Claim 7 has been added by way of this reply. Specifically, claim 7 recites a system including a communication device and a smart card device for calculating the hash function of a message. No new matter has been added by way of this amendment as support for this amendment

may be found, for example, in paragraphs [0021] – [0042] of the referenced application as published (*see* US 2006/0041568).

### **Amendments to the Drawings**

Figures 3 and 4 have been amended by way of this reply. The amended figures now show the reference character “R,” which represents the intermediate result of a hashing operation. No new matter has been added by way of this amendment, as support for this amendment may be found, for example, in paragraphs [0032] – [0035] of the referenced application as published.

### **Amendments to the Specification**

The specification has been amended to clarify the interaction between the mobile phone and the smart card. Specifically, the sentence “[t]hen, the mobile ME sends the intermediate result R and the remaining secret data SD to the smart card CAR” in paragraph [0032] has been amended to remove the phrase “and the remaining secret data SD.” Applicant submits that the phrase was included by mistake. This amendment is consistent with the operation of the invention recited throughout the Specification, for example, in paragraphs [0023] – [0024] and in the original claims 1 and 5.

### **Objections**

The Examiner objects to the specification for not including any reference signs. The Examiner also objects to the Drawings for failing to comply with 37 CFR 1.84(p)(5) with the assertion that there are no reference signs in Figures 1 – 4, because the Specification does not

include reference signs in the detailed description section. Applicant respectfully points out that the Specification does include reference characters that refer to elements in Figures 1 – 4. For example, in Figure 1, S refers to a system, ME refers to a mobile phone, CAR refers to a smart card, SERV refers to a server, and RES refers to a network. In Figures 2 – 4, MF refers to message, PD refers to public data, SD refers to secret data, RP refers to remaining part of last hash block, and SDC refers to secret data within a data block.

Applicant submits that the reference character “R” recited in the specification was not shown in the Figures 3 and 4 as originally filed. As discussed above, Figures 3 and 4 have been amended to include the reference character R. Thus, Applicant believes that all the reference characters now shown in the Figures 1 – 4 are mentioned in the description and that all the reference characters mentioned in the description are shown in Figures 1 – 4. Accordingly, withdrawal of this objection is respectfully requested.

### **Rejections under 35 U.S.C. § 102**

Claims 1 – 6, stand rejected under 35 U.S.C. § 102 (e) as being anticipated by WO 02/054663 (hereinafter “Quick”). Claim 3 has been canceled by way of this reply. Thus, this rejection is now moot with respect to canceled claim 3. To the extent that this rejection still applies to the remaining amended claims, the rejection is respectfully traversed.

One or more embodiments of the invention are directed to a method for calculating a hash of a message in a smart card and in a mobile phone. The message comprises secret data (*e.g.*, keys) and public data (*e.g.*, handshake data). For security, the keys are only known by the smart card, and are not communicated to the mobile phone.

The following discussion describes one or more embodiments of the invention. The discussion is included to the aid the Examiner in the understanding of one or more embodiments of the invention. However, the discussion is not intended to limit the scope of the claims.

Turning to the example, Figure 3 shows a message MF that includes a public data portion PD and a secret keys portion SD. The mobile phone ME starts calculating the hash of all the blocks that include PD. If there is a data block that includes both PD and SD, then the ME does not compute the hash of this block. Instead, the ME sends the intermediate results R (*i.e.*, the hash of all the preceding data blocks, which included only PD), along with the remaining public data RP to the smart card SC. The SC continues to calculate the hash internally by using the intermediate result R, the RP and the SD (*see* paragraph [0033] of the referenced application as published).

If the SD precedes the PD, as shown for example in Figure 4, then the SC starts the hashing of the message first. The SC calculates the hash of all the data blocks that include secret data SD. Figure 4 shows a data block that includes both SD and PD, which is also hashed by the SC. The resulting intermediate result R is then sent to the ME, which continues the hash calculation by using R and the remaining PD.

In the above discussed embodiments, both the SC and the ME only carry out a hashing of the respective input data. No signature of the input data is generated. In addition, all the keys, *i.e.*, SD, never leaves the smart card SC. Further, hashing of the blocks of data that include only public data is carried out exclusively in the ME, while hashing of the blocks that include SD is carried out exclusively on the SC.

Turning to the rejection, for anticipation under 35 U.S.C. § 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught

must be inherently present (See M.P.E.P. § 2131). From the above discussion and the reasons set forth below, Applicant believes that Quick fails to show or disclose all the limitations of the amended claims 1, 5 and 6. Specifically, Quick at least fails to teach at least the following limitations of the claims: (i) the secret data does not leave the smart card, (ii) a requesting step and a hashing step performed by the program on the communication device, and (iii) a program on the smart card for performing, when requested by the communication device, the step of hashing all keys of the message. Each of these limitations is discussed below.

**(i) Secret data not secured in the smart card**

Claims 1, 5, and 6 clearly recite, *inter alia*, "...the message is divided in data block and comprises keys and public data, and wherein the keys are *only known* by the smart card; ... " (emphasis added). In contrast, Quick shows a method in which secure authentication is provided to a user roaming outside his or her home system. Specifically, FIG. 3, of Quick shows a token 230 comprising a secure key 300, a key generator 250 and a signature generator 360. The user is authenticated to the visited system 210 by first sending a challenge to the token 230. The response generated by the token is verified by the visited system 210. In addition, the key generator 250 generates a cryptographic key (CK) 290, an integrity key (IK) 310, and a UIM authentication key (UAK) 320. The keys CK 290 and IK 310 are conveyed to the mobile unit 220 (*see* Quick, page 11, lines 8 – 14). Thus, contrary to the embodiments of the invention, as recited in claims 1, 5, and 6, the token (or smart card) 230 of Quick allows secret data, keys IK 310 and CK 290, to leave the token 230.

From the above it is clear that Quick clearly shows that the keys stored in the token 230 are communicated to the mobile unit 220 and, therefore, are known by both the token 230 and the mobile unit 220. Thus, Quick does not disclose at least this limitation of the independent claims 1, 5, and 6.

**(ii) No requesting step and hashing step**

Claim 5 of the application recites, *inter alia*, a hashing step in which all or part of said public data is hashed in said communication device, and a requesting step in which, the communication device requests the smart card to perform the hash function of the keys. In contrast, Quick discloses a communication device that may be coupled with a smart card, where the communication device comprises a program merely for calculating the authentication signature of a message including keys and other data. Specifically, FIG. 3 of Quick shows a signature generator 330 of the mobile unit generating a signature 340 based on the message 350 and the key IK 310. The signature signal 340 is transmitted to the subscriber identification token 230. At the subscriber identification token 230, the signature signal 340 and the UAK 320 are manipulated by a signature generator 360 to generate a primary signature 370. The program disclosed by Quick does not show the requesting step (for hashing all keys in the smart card) nor the hashing step (for hashing all or part of the public data in the device) as recited in claim 5. Therefore, Quick fails to disclose at least this limitation of claim 5.

**(iii) No Program on smart card to perform hashing on request from communication device**

Claim 6 of the invention recites, *inter alia*, a smart card that includes a program for performing, upon a request from the communication device, a hashing of the keys of the message. In contrast, Quick discloses a token 230 coupled with a mobile unit 220. The token 230 comprises of a signature generator 360 that receives a signature 340 from the mobile unit 220. However, Quick does not disclose a program for performing, when requested by the communication device, the step of hashing all keys of the message. In contrast, Quick discloses a program where weights of importance are assigned to messages so that only important messages are securely encrypted and authenticated (*see* Quick, page 13, lines 1 – 15). Thus, Quick does not disclose, at least this limitation of independent claim 6.

From the above discussion, it is evident that Quick does not disclose all the limitations of claims 1, 5, and 6. Thus, these claims are patentable over Quick. Claims 2 and 4 depend from claim 1, and are patentable for at least the same reasons as claim 1. Accordingly, withdrawal of this rejection is respectfully requested.

#### **New Claim**

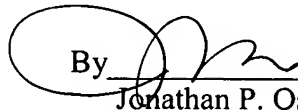
Independent claim 7 recites at least the same subject matter recited in independent claims 5 and 6 discussed above. Therefore, claim 7 is patentable over Quick for at least the same reasons as stated above with respect to claims 5 and 6. Accordingly, favorable action in the form of a Notice of Allowability is respectfully requested for new claim 7.

**Conclusion**

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 09669/054001).

Dated: April 18, 2007

Respectfully submitted,

By   
Jonathan P. Osha  
Registration No.: 33,986  
OSHA · LIANG LLP  
1221 McKinney St., Suite 2800  
Houston, Texas 77010  
(713) 228-8600  
(713) 228-8778 (Fax)  
Attorney for Applicant

Attachments:

Replacement sheet (Fig. 3 and Fig. 4)